UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/328,726	10/26/1998	THOMAS COLLINS	2026-25(PT-TA 410(Contl)	7212

7590 01/30/2004

HEWLETT-PACKARD COMPANY
Attn: Bill Streeter
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SEAL, JAMES	
ART UNIT	PAPER NUMBER
2135	30

DATE MAILED: 01/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/328,726	**Applicant(s)** COLLINS ET AL.	
	Examiner James Seal	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 06 November 2003.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 17-66 and 73-112 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 17-66 and 73-112 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 08/784453.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.

4) ☐ Interview Summary (PTO-413) Paper No(s). _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 06 November 2003.

2. Claims 1-16 have been cancelled without prejudice.

3. Claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 have been amended.

4. Claims 93-112 are new claims

5. Claims 17-66 and 73-112 are pending.

Specification

6. The new title " A Multiprime RSA Public Key Cryptosystem" is acceptable.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public –Key Cryptosystem, 1982) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest.

10. As per claim 17, the limitation of a cryptographic system which breaks messages into blocks M of size $0 \leq M \leq n$ where n is a modulus of an RSA encryption algorithm

$C \equiv M^e \bmod n$

$M \equiv C^d \bmod n$

$ed \equiv 1 \bmod \lambda(n)$

the latter would imply

$d \equiv e^{-1} \bmod \lambda(n)$

such that $n \in Z$ with prime factorization

$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$

$\lambda(n) = \mathrm{lcm}\,\{ \lambda(p_1^{e_1})\lambda(p_2^{e_2})\lambda(p_3^{e_3}) \ \ldots \ \lambda(p_k^{e_k})\}$

for which if $e_i > 2$

$\lambda(p_i^{e_i}) = \phi(p_i^{e_i})$

is the Euler totient and if $e_i = 1$

$\phi(p_i) = p_i - 1$

with e relatively primed to $(p_1-1)(p_2-1)(p_3-1) \ldots (p_k-1)$ which would imply

$d \equiv e^{-1} \bmod \{(p_1-1)(p_2-1)(p_3-1) \ldots (p_k-1)\}$

Is disclosed in Lidl page 289, lines 3, 5-6, bottom page 290, page 291 lines 3-7, page 293 problem 11. Lidl does not disclose the use of the Chinese Remainder Theorem (CRT) with respect to the problem at hand; however, by way of example, Lidl does teach application of his teachings to the special case of where the prime factors are distinct $p_1 = p$ and $p_2 = q$, that is, $e_1 = e_2 = 1$.

Quisquater teaches reduction RSA (two prime factors p and q) calculation to a simultaneous system of modular congruences

$C_1 \equiv C \bmod p_1$	$C_2 \equiv C \bmod p_2$
$M_1 \equiv C_1^{d_1} \bmod p_1$	$M_2 \equiv C_2^{d_2} \bmod p_1$
$d_1 \equiv d \bmod (p_1-1)$	$d_2 \equiv d \bmod (p_2-1)$

Solving for the results for M_1 and M_2 and combining the sub-task to produce the receive message M. Reducing the calculations to simultaneous sub-task allows Quisquater to carry out the calculations much faster as p_1 and p_2, d_1, d_2, M_1 M_2 and C_1 C_2 are much smaller in terms of the number of bits (see page 906 lines 3-8, 31-39, 55-60). Further such subtasks may be applied in parallel (see parallel below (1), "moreover the two computations may be done in parallel" and figure 1, for example the exponentiation modules x^2 mod p and x^2 mod q which calculate different subtasks at the same time. Thus one of ordinary skill in the art would recognize the speed and savings in computational resources which could be derived from using the teachings of Quisquater and would be strongly motivated to apply these teaching to Lidl algorithm. Lidl pages 515-517 also teaches the generalization of the above process for the case of k factors.

Lidl is silent on the choice of the e_i 's, as he is seeking to generalize the RSA system to its fullest. The RSA paper teaches both *randomness* and *distinctness* are important in the selection of primes for the two prime factors p and q scheme that they propose (see Rivest et. al. page 6, line 34 ;page 9, lines 2-3, and line 26-27) in order to maximize security. If the size of the modulus n is restricted to 200 digits, then maximum security is attained by taking by choose p and q differing by a few digits (distinctness) and choosen at random. Thus if randomness and distinctness is not applied to multifactor scheme, one losses the randomness that is there are a lot fewer ways to choose a two hundred digit number of the form p^2 q as opposed to pqr and hence a loss of security. Thus one of ordinary skill in the art would recognize in order to maximize security one must increase the number of possible choices which implies distinctness of all factors that is $e_1 = e_2 = e_3 = \ldots = e_k$ in the teaching of Lidl. Thus one of ordinary skill of the art would have been motivated to combine the general teachings of Lidl with the additional speed enhancements of Quisquater and finally the security teachings of the original RSA paper to obtain a security system which is fast and could run on devices with limited computational resources such as CD ROM's, smartcards, secure net browers, etc. Claim 17 is rejected.

Claim 18-66 and 73-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Lidl and Pilz (Applied Abstract Algebra, 1984), and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public –Key Cryptosystem, 1982) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et. al. The Chinese Remainder Theorem, World Scientific.

7. As per claim 18-21, the details of a recursive (iterative) algorithm is given page 23. Note the relabling of the dummy indices and the use of the extended Euclidian algorithm $u_iM_i + v_i m_i = 1$ to provide the inverse u_i or w^{-1}_i modulo m_k or p_i in 2.8 of the product M_k corresponding to applicant's w_i . Claims 18-21 are rejected.

8. Claims 22-26 are a system implementation of claims 17-21 and are rejected in view of the same prior art of record.

9. In claim 17, the limitation of the decomposition into subtasks performed simultaneously, of the RSA decryption equation was applied without any corresponding

application of the same technique to the encryption part of the encryption system. The limitations of claims 27 are directed to the same decomposition into subtasks to be performed simultaneously. One of ordinary skill in the art recognizing the same benefits may be had by applying the same mathematics to the encryption area would have been motivated to apply it to the encryption part of the cryptosystem to gain the same benefits. Claim 27 is rejected.

10. As per claims 28-31, expand upon the CRT algorithm applied to this aspect of the encryption and would be rejected on the same group as claims 18-21. Claims 28-31 are rejected.

11. Claims 32-36 are a system implementation of claims 27-31 and are rejected in view of the same prior art of record. Claims 27-31 are rejected.

12. Claims 37-41 and 44 recite a method for decoding corresponding to the method of encoding claims of 17-22 and are rejected in view of the same prior are (all refereneces disclosed both an encoding and decoding scheme). Claim 37-41 and 44 are rejected.

13. As per claims 42-43, and 45-46, the limitation of a cryptographic system for decoding implementing method of claims 37-41, and 44 is rejected in view of the same prior art of record. Claims 42-41 and 44 are rejected.

14. As per claim 47-51, the limitation for a method of generating digital signature is disclosed by Rivest (see pages 4-6) for two prime factors. Using the Lidl/Quisquater/Ding scheme, one of ordinary skill in the art would have also been modivated to apply the same techniques to digital signature to increase speed, conserve computational resources which

are important credit card transactions, and digital rights management. Claims 47-51 are rejected.

15. Claims 52-56 are a system implementation for the generating method recited in claims 47-52 and is rejected in view of the same prior art of record. Claims 52-56

16. As per claims 57-61, the limitations of a process for verifying digital signatures, recited in the method claims 47-52 is disclosed by Rivest (page 5). Claims 57-61 are rejected.

17. Claims 62-66, recite a system for generating and validating digital signatures corresponding to method claims 47-51 and 57-61 and are rejected in view of the same prior art of record.

18. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 recites the limitation of a plurality of exponentiator units operating substantially simultaneously and performing subtasks are disclosed by Figure 1 Quisquater. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 are rejected.

19. Claims 74, 76, 78, 80, 82, 84, 86, 88, 90, 92 recite the limitation that each distinct random prime factore has the same number of bits is disclosed in Quisquater page 906 second column under figure 1.

20. Claims 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et. al. (US 4,405,829 A) henceforth RSA, and further in view of Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest, Quisquater, Fast Decipherment Algorithm for RSA

Public-key Cryptosystem and further in view of Knuth, The Art of Computer Programming vol 2 page 179.

21. As per claim 17, the limitation of a method for processing messages in a communication system with RSA public key encryption an alternative embodiment of the present invention (see Figure 6, Abstract line 1 of Column 4, lines 15 through Column 5, lines 11, RSA), such that three or more primes $p_1, p_2, p_3, \ldots, p_k$ are generated, such that $k > 2$ (Column 13, lines 30-31) then using the present invention (Column 13, line 29) provided and e relatively prime to $\phi(n)$ (Column 13, lines 42-44), $\phi(n) = (p_1-1)(p_2-1)(p_3-1)\ldots(p_k-1)$, that is, relatively prime to $(p_1-1)(p_2-1)(p_3-1)\ldots(p_k-1)$ and generating from the product of these primes and integer n which will be the resulting modulus n (Column 13, line 30-31, line 34) using the provided e and n together with a message M where $0 \leq M \leq n-1$ (Column 4, line 26), and the RSA encryption algorithm $C \equiv M^e \bmod n$ (Column 4, line 59, RSA) to generate a cipher text C, decrypting C at the intended recipient (Column 6, 29-31) having available to it. RSA suggest the CRT but is silent on the details. Quisquater provides the details and motivations (see discussion in claim 17 above) for the implementation for two parameters.

22. The RSA paper teaches both *randomness* and *distinctness* are important in the selection of primes for the two prime factors p and q scheme that they propose (see Rivest et. al. page 6, line 34 ;page 9, lines 2-3, and line 26-27) in order to maximize security. If the size of the modulus n is restricted to 200 digits, then maximum security is attained by taking by choose p and q differing by a few digits (distinctness) and chosen at random. Thus if randomness and distinctness is not applied to multifactor scheme, one losses the randomness that is there are a lot fewer ways to choose a two

hundred digit number of the form p^2 q as opposed to pqr and hence a loss of security. Thus one of ordinary skill in the art would recognize in order to maximize security one must increase the number of possible choices which implies distinctness of all factors that is $e_1 = e_2 = e_3 = \ldots = e_k$. Thus one of ordinary skill of the art would have been motivated to combine the general teachings of Lidl with the additional speed enhancements of Quisquater and finally the security teachings of the original RSA paper to obtain a security system which is fast and could run on devices with limited computational resources such as CD ROM's, smartcards, secure net browsers, etc.

23. RSA patent recites a different embodiment (Column 13, lines 30-31) in which the modulus n is a product of three or more primes (not necessarily distinct primes). RSA further goes on to state that decoding may be performed modulo each of the prime factors of n (thus breaking the calculations into a series of subtasks involving the factors of n and not n) and then combining the results using "Chinese remaindering" (that is the Chinese remainder theorem henceforth CRT). However, only in the case of distinct primes can the decoding problem be performed using the CRT. In the case of non-distinct primes one would need in addition Hensel's Lemma (or a generalization by Hensel of p-adics, see Knuth vol 2, page 179). Thus it is clear that the RSA patent is referring to the case of distinct primes. Claim 1 is rejected.

24. Claim 18-66 and 73-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et. al. (US 4,405,829 A) henceforth RSA, and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public –Key Cryptosystem, 1982) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key

Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et. al. The Chinese Remainder Theorem, World Scientific.

25. As per claim 18-21, the details of a recursive (iterative) algorithm is given page 23. Note the relabling of the dummy indices and the use of the extended Euclidian algorithm $u_iM_i + v_i m_i = 1$ to provide the inverse u_i or w^{-1}_i modulo m_k or p_i in 2.8 of the product M_k corresponding to applicant's w_i . Claims 18-21 are rejected.

26. Claims 22-26 are a system implementation of claims 17-21 and are rejected in view of the same prior art of record.

27. In claim 17, the limitation of the decomposition into subtasks performed simultaneously, of the RSA decryption equation was applied without any corresponding application of the same technique to the encryption part of the encryption system. The limitations of claims 27 are directed to the same decomposition into subtasks to be performed simultaneously. One of ordinary skill in the art recognizing the same benefits may be had by applying the same mathematics to the encryption area would have been motivated to apply it to the encryption part of the cryptosystem to gain the same benefits. Claim 27 is rejected.

28. As per claims 28-31, expand upon the CRT algorithm applied to this aspect of the encryption and would be rejected on the same group as claims 18-21. Claims 28-31 are rejected.

29. Claims 32-36 are a system implementation of claims 27-31 and are rejected in view of the same prior art of record. Claims 27-31 are rejected.

30. Claims 37-41 and 44 recite a method for decoding corresponding to the method of encoding claims of 17-22 and are rejected in view of the same prior are (all refereneces disclosed both an encoding and decoding scheme). Claim 37-41 and 44 are rejected.

31. As per claims 42-43, and 45-46, the limitation of a cryptographic system for decoding implementing method of claims 37-41, and 44 is rejected in view of the same prior art of record. Claims 42-41 and 44 are rejected.

32. As per claim 47-51, the limitation for a method of generating digital signature is disclosed by Rivest (see pages 4-6) for two prime factors. Using the Lidl/Quisquater/Ding scheme, one of ordinary skill in the art would have also been modivated to apply the same techniques to digital signature to increase speed, conserve computational resources which are important credit card transactions, and digital rights management. Claims 47-51 are rejected.

33. Claims 52-56 are a system implementation for the generating method recited in claims 47-52 and is rejected in view of the same prior art of record. Claims 52-56

34. As per claims 57-61, the limitations of a process for verifying digital signatures, recited in the method claims 47-52 is disclosed by Rivest (page 5). Claims 57-61 are rejected.

35. Claims 62-66, recite a system for generating and validating digital signatures corresponding to method claims 47-51 and 57-61 and are rejected in view of the same prior art of record.

36. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 recites the limitation of a plurality of exponentiator units operating substantially simultaneously and performing subtasks are

disclosed by Figure 1 Quisquater. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 are rejected.

37. Claims 74, 76, 78, 80, 82, 84, 86, 88, 90, 92 recite the limitation that each distinct random prime factor has the same number of bits is disclosed in Quisquater page 906 second column under figure 1.

38. Claim 17 is rejected under 35 U.S.C. 103(a) in view of Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996 and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest and Quisquater Fast Decipherment Algorithm for RSA Public-key Cryptosystem, 1982.

39. Nemo discloses the use of a three prime RSA (see section 3). Each prime p, q, r would contain the same number of bits (256 bits) and the modulus n would contain 768 bits. The system would provide digital signature, encryption, decryption, and self encryption (files, backup tapes and archives) and in section 4.2 provide secure signed routers for networks. Nemo's three prime RSA is faster because of the CRT(section 3.1). Although, Nemo's three prime RSA applies CRT to decryption section, still greater speed could be achieved by applying to both encryption/decryption. Such details are supplied by Quisquater.

40. The RSA paper teaches both *randomness* and *distinctness* are important in the selection of primes for the two prime factors p and q scheme that they propose (see Rivest et. al. page 6, line 34 ;page 9, lines 2-3, and line 26-27) in order to maximize security. If the size of the modulus n is restricted to 200 digits, then maximum security

is attained by taking by choose p and q differing by a few digits (distinctness) and choosen at random. Thus if randomness and distinctness is not applied to multifactor scheme, one losses the randomness that is there are a lot fewer ways to choose a two hundred digit number of the form p^2 q as opposed to pqr and hence a loss of security. Thus one of ordinary skill in the art would recognize in order to maximize security one must increase the number of possible choices which implies distinctness of all factors that is $e_1 = e_2 = e_3 = \ldots = e_k$. Thus one of ordinary skill of the art would have been modivated to combine the general teachings of Lidl with the additional speed enhancements of Quisquater and finally the security teachings of the original RSA paper to obtain a security system which is fast and could run on devices with limited computational resources such as CD ROM's, smartcards, secure net browers, etc. Claim 17is rejected.

41. Claim 18-66 and 73-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Nemo, RSA Moduli Should Have 3 Primes Factors, August 1996, and further in view of Quisquater and Couvreur, Fast Decipherment Algorithm for RSA Public –Key Cryptosystem, 1982) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, as applied to claim 17 above, and further in view of Ding et. al. The Chinese Remainder Theorem, World Scientific.

42. As per claim 18-21, the details of a recursive (iterative) algorithm is given page 23. Note the relabling of the dummy indices and the use of the extended Euclidian

algorithm $u_iM_i + v_i m_i = 1$ to provide the inverse u_i or w^{-1}_i modulo m_k or p_i in 2.8 of the product M_k corresponding to applicant's w_i . Claims 18-21 are rejected.

43. Claims 22-26 are a system implementation of claims 17-21 and are rejected in view of the same prior art of record.

44. In claim 17, the limitation of the decomposition into subtasks performed simultaneously, of the RSA decryption equation was applied without any corresponding application of the same technique to the encryption part of the encryption system. The limitations of claims 27 are directed to the same decomposition into subtasks to be performed simultaneously. One of ordinary skill in the art recognizing the same benefits may be had by applying the same mathematics to the encryption area would have been motivated to apply it to the encryption part of the cryptosystem to gain the same benefits. Claim 27 is rejected.

45. As per claims 28-31, expand upon the CRT algorithm applied to this aspect of the encryption and would be rejected on the same group as claims 18-21. Claims 28-31 are rejected.

46. Claims 32-36 are a system implementation of claims 27-31 and are rejected in view of the same prior art of record. Claims 27-31 are rejected.

47. Claims 37-41 and 44 recite a method for decoding corresponding to the method of encoding claims of 17-22 and are rejected in view of the same prior are (all refereneces disclosed both an encoding and decoding scheme). Claim 37-41 and 44 are rejected.

48. As per claims 42-43, and 45-46, the limitation of a cryptographic system for decoding implementing method of claims 37-41, and 44 is rejected in view of the same prior art of record. Claims 42-41 and 44 are rejected.

49. As per claim 47-51, the limitation for a method of generating digital signature is disclosed by Rivest (see pages 4-6) for two prime factors. Using the Lidl/Quisquater/Ding scheme, one of ordinary skill in the art would have also been modivated to apply the same techniques to digital signature to increase speed, conserve computational resources which are important credit card transactions, and digital rights management. Claims 47-51 are rejected.

50. Claims 52-56 are a system implementation for the generating method recited in claims 47-52 and is rejected in view of the same prior art of record. Claims 52-56

51. As per claims 57-61, the limitations of a process for verifying digital signatures, recited in the method claims 47-52 is disclosed by Rivest (page 5). Claims 57-61 are rejected.

52. Claims 62-66, recite a system for generating and validating digital signatures corresponding to method claims 47-51 and 57-61 and are rejected in view of the same prior art of record.

53. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 recites the limitation of a plurality of exponentiator units operating substantially simultaneously and performing subtasks are disclosed by Figure 1 Quisquater. Claims 73, 75, 77, 79, 81, 83, 85, 87, 89, 91 are rejected.

54. Claims 74, 76, 78, 80, 82, 84, 86, 88, 90, 92 recite the limitation that each distinct random prime factor has the same number of bits is disclosed in Quisquater page 906 second column under figure 1.

55. As per new dependent claims 93-112, claims 93, 95, 97, 99, 101, 103, 105, 107, 109, and 111recite the limitation that a plurality of k sub-tasks are performed in parallel is

taught by Quisquater and Couvreur. As noted in their paper "Fast Decipherment Algorithm For RSA Public-key Cryptosystem (the paragraph below equation (1)) "Moreover the two computations may be done in parallel" thus teaching the CRT as a means of parallel processing. Claims 93, 95, 97, 99, 101, 103, 105, 107, 109, and 111 are rejected. Claims 94, 96, 98, 100, 102, 104, 106, 108, 110, and 112 recite the further limitation wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT) is taught by Quisquater and Couvreur (see sentence above (1)). Claims 94, 96, 98, 100, 102, 104, 106, 108, 110, and 112 are rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Response to Arguments

56. Applicant's arguments with respect to claim 17-66 and 73-112 have been considered but persuasive.

57. With regards to Nemo, RSA Moduli Should Have 3 Prime Factors, © August 1996 (as per footnote page 1), Applicant asserts that the Captain Nemo paper cannot

be accreted as being published on August 1996 since the paper was submitted under a pseudonym and under what appears to be a fictitious publication name "Scientific Bulgarian". However Applicant's argument relies on the false assumption is a fictitious publication renders no meaning to the stated publication date August 1996. On the contrary "scientific Bulgarian" is well known in the art as a indication of a paper being published under, "Copyleft for scientific papers" (see citations's), As can be seen, the first footnote of the Captain Nemo paper fully complies with the directives of copyleft, and thus fully must be accepted as valid evidence that the Captain Nemo paper was indeed published August 1996. Further note that academia is replete with many pseudonyms without detracting from their validity e.g. "Publius" as author of *The Federalist*, "Anon et. al." as the original author of the Transaction Processing Benchmark Papers (It evolved from the DebitCredit test originally published in 1984. This effort was spearheaded by Jim Gray but had so many contributors from industry and academia that the author on the paper was given as Anon et al. This paper struck a chord in the database community.), "Nicholas Bourbaki" the famous French formalist mathematical school and was a Professor at the University of "Nanciago" (as many of its members that wrote of the pseudonym of Bourbaki were from the University of Nance and the University of Chicago) and final "Student" (for William Sealey Gosset the famous statistician of Guinness Brewery).

58. With regards to the Applicant's argument that the "examiner picks and chooses various portions of the three publications (Lidl, Applied Abstract Algebra 1984, Quisquater and Courreur, Fast Decipherment Algorithm for RSA Public-kkey

Cryptosystem, 1982, Rivest et. al. A method for obtaining Digital Signatures and Public-key Cryptosystem) to piece together the subject matter of the present claims" It should be noted that Rivest first suggest the method of using multiple primes and the CRT and Lidl (an undergraduate textbook) sets the steps out for the student and finally Quisquater and Courreur show how to apply it for a faster algorithm. Thus rather than "picking and choosing" various portions of prior art at random, examiner merely is following a direction originally motivated and set forth by Rivest (in Lidl).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 ~~9711~~ 4393. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

JWS

Jws
AU 2135
25 January 2004

[illegible]
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100